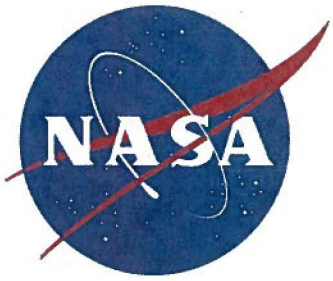

IT Security Handbook

Information System Security Plan Numbering Schema

ITS-HBK-0007B
Effective Date: 20100308
Expiration Date: 20120308
Responsible Office: OCIO/Deputy CIO for Information Technology Security

Contents

Approval

Jerry L. Davis
Deputy Chief Information Officer for
Information Technology Security

3/8/10
Date

Distribution:

NODIS

Change History

ITS-HBK-0007 System Security Plan Numbering Schema

Change Number	Date	Change Description
B	**3/8/2010**	**Change from ITS-SOP-0007B to ITS-HBK-0007B**

1. Purpose

1.1. This IT Security Handbook (ITS-HBK) establishes NASA's standard numbering schema for identifying Information System Security Plans (SSP). The schema retains the existing SSP Registry numbering, and links the unique identifier to the responsible Authorizing Official (AO) and the responsible Center.

1.2. This ITS-HBK applies to all personnel involved in the IT security of NASA information systems.

1.3. Applicable Documents.

a. FIPS 199 Standards for Security Categorization of Federal Information and Information Systems.

b. NPR 2810.1 Security of Information Technology.

2. Roles and Responsibilities

2.1. The Information System Owner (ISO) assigns all portions of the security plan numbering schema and uses this ITS-HBK as guidance to ensure the applicable fields are assigned appropriately.

2.2. Security Documentation Creator/Preparer ensures that the security plan numbering schema fields are entered into the NASA System Assessment and Authorization Repository (NSAAR) appropriately and updated as necessary.

3. Process

3.1. **Security Plan Numbering Schema**

3.1.1. All IT system security plans shall have a unique identifier that consists of multiple fields separated by hyphens: AA-mmm-a-bbb-nnnn

3.2. An explanation of each field is:

3.2.1. [AA] - This is a two letter field that identifies the functional office that is responsible for the system security plan. There are currently 21 possible functional offices and sub-offices with Authorizing Officials that can accredit NASA information systems. Accordingly, this field must have one of the following values:

AR	Aeronautics Research Mission Directorate
CD	Multi-Program systems which support multiple Mission Directorates (authorized by the Center Deputy Director or Center CIO)
ED	Chief Education Officer
EG	Office of the Chief Engineer
ER	External Relations
EX	Exploration Systems Mission Directorate
FO	Office of the Chief Financial Officer
GC	Office of General Counsel
HM	Office of Chief Health and Medical Officer
IE	Integrated Enterprise Management Program
IG	Office of Inspector General

IM Institutions and Management Mission Support Directorate
IO Office of Chief Information Officer
IP Innovative Partnership Program
OA Office Automation Information Technology (OAIT)
OS Office of Security and Program Protection
PA Office of Program Analysis and Evaluation
PI Program and Institutional Integration
SC Science Mission Directorate
SO Space Operations Mission Directorate
SP Office of Safety and Mission Assurance Systems
NN External (Non-NASA) Systems (Contains/processes NASA information.)

3.2.2. [mmm] - This is a three digit numeric field that can be used to identify the system within a Center. If a Center chooses not to utilize this field for internal organizational identification, this number can default to '999'.

3.2.3. [a] This is a single letter field that identifies the FIPS-199 security categorization of the system:

L – Indicates the system is Low
M – Indicates the system is Moderate
H – Indicates the system is High

3.2.4. [bbb] - This is a three letter field that identifies the Center that is responsible for tracking the system. This is usually where the system is located, managed, or reported. There are 12 possible values for this field, as follows:

ARC Ames Research Center
DFR Dryden Flight Research Center
GRC Glenn Research Center
GSF Goddard Space Flight Center
JPL the Jet Propulsion Laboratory
JSC Johnson Space Center
KSC Kennedy Space Center
LRC Langley Research Center
MSF Marshall Space Flight Center
NHQ NASA Headquarters
NSS NASA Shared Services Center
SSC Stennis Space Center

3.2.5. [nnnn] - This is a four digit numeric field that identifies the system.

3.3. **Examples:**

3.3.1. OA-101-L-DFR-1002 - This is an example of a valid system security plan number for an OAIT LAN System located at the Dryden Flight Research Center.

3.3.2. SO-999-L-KSC-6601 - This is an example of a valid system security plan number for a Space Operations system located at Kennedy Space Center.

Appendix A. Definitions

High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. [FIPS 200]
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Information	An instance of an information type. [FIPS 199]
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]
Information System (Also referred to as IT System)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[44 U.S.C., Sec. 3502] (Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) [NIST]
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST; CNSS 4009, Adapted)
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. [40 U.S.C., Sec. 1401]
Information Technology (IT) System	See information system.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined

	by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]
Low-Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. [FIPS 200]
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. [FIPS 200]
NASA Information	Any knowledge that that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for, or is under the control of NASA. [NPD 2810.1D]
Security	Security is a system property. Security is much more that a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms, which span the system both logically and physically.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. [NIST] See *System Security Plan* or *Security Program Plan.*
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]

Appendix B. Acronyms

AO	Authorization Official
FIPS	Federal Information Processing Standards
HBK	Handbook
ISO	Information System Owner
LAN	Local Area Network
NSAAR	NASA System Assessment and Authorization Repository
OAIT	Office Automation Information Technology
ITS	Information Technology Security
SSP	System Security Plan